Configuration, initiale et pour l'accès client à distance, du concentrateur Cisco VPN 5000

Contenu

Introduction

Ce guide explique la configuration initiale du concentrateur de Cisco VPN 5000, spécifiquement comment le configurer pour se connecter au réseau utilisant l'IP, et offre la Connectivité de client distant.

Vous pouvez installer le concentrateur dans l'un ou l'autre de deux configurations, selon où vous le connectez au réseau par rapport à un Pare-feu. Le concentrateur a deux ports Ethernet, l'un d'entre eux (le trafic d'IPSec de passages d'Ethernets 1) seulement. L'autre port (Ethernet 0) conduit tout le trafic IP. Si vous prévoyez d'installer le concentrateur VPN parallèlement au Pare-feu, vous devez utiliser les deux ports de sorte que l'Ethernet 0 fasse face au RÉSEAU LOCAL protégé, et l'Ethernet 1 fasse face à l'Internet par le routeur de passerelle Internet du réseau. Vous pouvez également installer le concentrateur derrière le Pare-feu sur le RÉSEAU LOCAL protégé et le connecter par le port d'Ethernet 0, de sorte que le trafic d'IPSec passant entre l'Internet et le concentrateur soit traversé le Pare-feu.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur le concentrateur de Cisco VPN 5000.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration de base de Connectivité

Le moyen le plus simple d'établir la connexion réseau de base est de connecter un câble série au port de console sur le concentrateur et d'employer le logiciel de terminal pour configurer l'adresse IP sur le port d'Ethernet 0. Après avoir configuré l'adresse IP sur le port d'Ethernet 0, vous pouvez employer le telnet pour se connecter au concentrateur pour se terminer la configuration. Vous pouvez également générer un fichier de configuration dans un éditeur de texte compétent, et l'envoyez au concentrateur utilisant le TFTP.

Utilisant le logiciel de terminal par le port de console, vous êtes au commencement incité pour un mot de passe. Utilisez le mot de passe « letmein. » Après avoir répondu avec le mot de passe, émettez la commande d'**Ethernet 0 d'IP de configurer**, répondant aux demandes avec vos informations système. L'ordre des demandes devrait ressembler à ceci :

```
*[ IP Ethernet 0 ]# configure ip ethernet 0
      Section 'ip ethernet 0' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IP Ethernet 0 ]# ipaddress=192.168.233.1
      *[ IP Ethernet 0 ]# subnetmask=255.255.255.0
      *[ IP Ethernet 0 ]# ipbroadcast=192.168.233.255
      *[ IP Ethernet 0 ]# mode=routed
      *[ IP Ethernet 0 ]#
```

Maintenant vous êtes prêt à configurer le port d'Ethernet 1.

Port d'Ethernet 1

Les informations d'adressage TCP/IP sur le port d'Ethernet 1 sont les externes, adresse TCP/IP d'Internet-routable que vous avez assignée pour le concentrateur. Évitez d'utiliser une adresse dans le même réseau TCP/IP que des Ethernet 0, car ceci désactivera le TCP/IP dans le concentrateur VPN.

Sélectionnez les commandes des **Ethernets 1 d'IP de configurer**, répondant aux demandes avec vos informations système. L'ordre des demandes devrait ressembler à ceci :

```
*[ IP Ethernet 0 ]# configure ip ethernet 1
      Section 'ip ethernet 1' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IP Ethernet 1 ]# ipaddress=206.45.55.1
      *[ IP Ethernet 1 ]# subnetmask=255.255.255.0
      *[ IP Ethernet 1 ]# ipbroadcast=206.45.55.255
      *[ IP Ethernet 1 ]# mode=routed
      *[ IP Ethernet 1 ]#
```

Maintenant vous le besoin de configurer le default route.

Default route

Vous devez configurer un default route que le concentrateur peut employer pour envoyer tout le trafic TCP/IP destiné pour des réseaux autres que les réseaux auxquels on le connecte directement, ou pour ce qu'il a les artères dynamiques. Le default route redésigne tous les réseaux trouvés sur le port interne. Plus tard, vous configurerez l'Intraport pour envoyer le trafic d'IPSec à et de l'Internet utilisant le paramètre de passerelle d'IPSec. Pour commencer la configuration de default route, sélectionnez la commande statique d'IP de config d'éditer, répondant aux demandes avec vos informations système. L'ordre des demandes devrait ressembler à ceci :

```
*IntraPort2+_A56CB700# edit config ip static
      Section 'ip static' not found in the config.
      Do you want to add it to the config? y
      Configuration lines in this section have the following format:
      <Destination> <Mask> <Gateway> <Metric> [<Redist=(RIP|none)>]
      Editing "[ IP Static ]"...
      1: [ IP Static ]
      End of buffer
      Edit [ IP Static ]> append 1
      Enter lines at the prompt. To terminate input, enter
      a . on a line all by itself.
      Append> 0.0.0.0 0.0.0.0 192.168.233.2 1
      Append> .
      Edit [ IP Static ]> exit
      Saving section...
      Checking syntax...
      Section checked successfully.
      *IntraPort2+_A56CB700#
```

Maintenant vous devez configurer la passerelle d'IPSec.

Passerelle d'IPSec

Les contrôles de passerelle d'IPSec où le concentrateur envoie tout l'IPSec, ou percé un tunnel, le trafic. C'est indépendant du default route que vous avez juste configuré. Début en écrivant la commande **générale de configurer**, répondant aux demandes avec vos informations système. L'ordre des demandes devrait ressembler à ceci :

```
* IntraPort2+_A56CB700#configure general
      Section 'general' not found in the config.
      Do you want to add it to the config? y
```

```
      Configure parameters in this section by entering:
       =
      To find a list of valid keywords and additional help enter "?"
      *[ General ]# ipsecgateway=206.45.55.2
      *[ General ]# exit
      Leaving section editor.
      * IntraPort2+_A56CB700#
```

Ensuite, configurez la stratégie IKE.

Stratégie IKE

Placez les paramètres de protocole de gestion de clés/échange de clés Internet (IKE) d'association de sécurité internet (ISAKMP/IKE) pour le concentrateur. Ces configurations contrôlent comment le concentrateur et le client identifient et s'authentifient afin d'établir des sessions de tunnel. Cette première négociation est mentionnée car phase les paramètres de 1. Phase 1 sont globaux au périphérique et ne sont pas associés avec une interface spécifique. Les mots clé identifiés dans cette section sont décrits ci-dessous. Des paramètres de négociation de Phase 1 pour des tunnels entre réseaux locaux peuvent être placés dans [<Section ID> de partenaire de tunnel] la section.

Contrôles de négociation d'IKE de Phase 2 comment le concentrateur et le client VPN manipulent différentes sessions de tunnel. Des paramètres de négociation d'IKE de Phase 2 pour le concentrateur et le client VPN sont placés dans [le périphérique de <Name> de groupe VPN]

La syntaxe pour la stratégie IKE est comme suit :

```
* IntraPort2+_A56CB700#configure general
      Section 'general' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
       =
      To find a list of valid keywords and additional help enter "?"
      *[ General ]# ipsecgateway=206.45.55.2
      *[ General ]# exit
      Leaving section editor.
      * IntraPort2+_A56CB700#
```

Le mot clé de protection spécifie une suite de protection pour la négociation ISAKMP/IKE entre le concentrateur VPN et le client. Ce mot clé peut apparaître de plusieurs périodes dans cette section, dans ce cas le concentrateur propose toutes les suites spécifiées de protection. Le client reçoit une des options pour la négociation. La première partie de chaque option, MD-5 (le message-digest 5), est l'algorithme d'authentification utilisé pour la négociation. Le SHA signifie le Secure Hash Algorithm, qui est considéré plus sécurisé que le MD5. La deuxième partie de chaque option est l'algorithme de chiffrement. DES (norme de chiffrement de données) emploie une clé 56-bit pour brouiller les données. La troisième partie de chaque option est le groupe de Diffie-Hellman, utilisé pour l'échange clé. Puisque de plus grands nombres sont utilisés par l'algorithme du groupe 2 (G2), il est plus sécurisé que le groupe 1 (G1).

Pour commencer la configuration, sélectionnez la commande de **stratégie IKE de configurer**, répondant aux demandes avec vos informations système.

```
* IntraPort2+_A56CB700# configure IKE policy
      Section 'IKE Policy' was not found in the config.
      Do you want to add it to the config? y
```

```
Configure parameters in this section by entering:
<Keyword> = <Value>
To find a list of valid keywords and additional help enter "?"
*[ IKE Policy ] Protection = MD5_DES_G1
*[ IKE Policy ] exit
Leaving section editor.
* IntraPort2+_A56CB700#
```

Maintenant que les fondements sont configurés, entrez les paramètres de groupe.

Configuration de groupe VPN

En écrivant des paramètres de groupe, souvenez-vous que le nom de groupe VPN ne devrait pas contenir les espaces, quoique le programme d'analyse syntaxique de ligne de commande te permette pour écrire les espaces dans le nom de groupe VPN. Le nom de groupe VPN peut contenir des lettres, des nombres, des tirets, et des traits de soulignement.

Il y a quatre paramètres de base qui sont exigés à chaque groupe VPN pour l'exécution IP :

- Maxconnections
- StartIPaddress ou LocalIPNet
- Transformez
- IPNet

Le paramètre de Maxconnections est le nombre maximal de sessions de client simultanées permises dans cette configuration particulière de groupe VPN. Maintenez ce nombre dans l'esprit, comme cela fonctionne en même temps que le paramètre de StartIPAddress ou de LocalIPNet.

Le concentrateur VPN assigne des adresses IP aux clients distants par deux schémas, StartIPAddress et LocalIPNet différents. StartIPAddress assigne des numéros IP du sous-réseau connecté aux Ethernet 0 et aux proxy-arp pour les clients connectés. LocalIPNet assigne des numéros IP aux clients distants d'un sous-réseau seul aux clients vpn, et a besoin de que le reste du réseau est mis au courant de l'existence du sous-réseau VPN par la charge statique ou le routage dynamique. StartIPAddress offre une configuration plus facile, mais peut limiter la taille de l'espace d'adressage. LocalIPNet offre la meilleure flexibilité de l'adressage pour des utilisateurs distants, mais exige de légèrement plus de travail de configurer le routage nécessaire.

Pour StartIPAddress, utilisez la première adresse IP assignée à une session de tunnel entrante de client. Dans une installation de configuration de base, ceci devrait être une adresse IP sur le réseau TCP/IP interne (le même réseau comme le port d'Ethernet 0). Dans notre exemple ci-dessous, la première session de client est assignée l'adresse de 192.168.233.50, la prochaine session de client simultanée est assignée 192.168.233.51, et ainsi de suite. Nous avons assigné une valeur de Maxconnections de 30, qui signifie que nous devons avoir un bloc de 30 adresses IP inutilisées (serveurs DHCP y compris si vous en avez) commençant par 192.168.233.50 et finissant avec 192.168.233.79. Avoid superposant les adresses IP utilisées dans différentes configurations de groupe VPN.

LocalIPNet assigne des adresses IP aux clients distants d'un sous-réseau qui doit être inutilisé ailleurs sur le RÉSEAU LOCAL. Par exemple, si vous spécifiez le paramètre "LocalIPNet=182.168.1.0/24" dans la configuration de groupe VPN, le concentrateur assigne des adresses IP aux clients commençant par 192.168.1.1. Par conséquent, vous devez assigner "Maxconnections=254", car le concentrateur n'observera pas des bornes de sous-réseau quand assignant des numéros IP utilisant LocalIPNet.

Le mot clé de transformation spécifie les types et les algorithmes de protection que le concentrateur utilise pour des sessions de client d'IKE. Les options sont comme suit :

```
* IntraPort2+_A56CB700# configure IKE policy
      Section 'IKE Policy' was not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IKE Policy ] Protection = MD5_DES_G1
      *[ IKE Policy ] exit
      Leaving section editor.
      * IntraPort2+_A56CB700#
```

Chaque option est une partie de protection qui spécifie l'authentification et les paramètres de chiffrement. Ce mot clé peut apparaître de plusieurs périodes dans cette section, dans ce cas le concentrateur propose les parties spécifiées de protection dans la commande qu'ils sont analysés, jusqu'à ce qu'une soit reçue par le client pour l'usage pendant la session. Dans la plupart des cas, seulement un transforment le mot clé est nécessaire.

L'ESP (SHA, DES), ESP(SHA,3DES), ESP(MD5,DES), et ESP(MD5,3DES) dénotent l'en-tête de Protocole ESP (Encapsulating Security Payload) pour chiffrer et authentifier des paquets. DES (norme de chiffrement de données) emploie une clé 56-bit pour brouiller les données. 3DES emploie trois clés différentes et trois applications de l'algorithme DES pour brouiller les données. Le MD5 est l'algorithme de hachage du message-digest 5, et le SHA est le Secure Hash Algorithm, qui est considéré en quelque sorte plus sécurisé que le MD5.

ESP(MD5,DES) est la valeur par défaut et est recommandé pour la plupart des installations. Utilisation d'ESP(MD5) et ESP(SHA) l'en-tête de l'ESP d'authentifier des paquets sans le cryptage. Utilisation d'AH(MD5) et AH(SHA) l'En-tête d'authentification (AH) d'authentifier des paquets. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES), et AH(SHA)+ESP(3DES) utilisation l'en-tête d'authentification d'authentifier des paquets et l'en-tête de l'ESP pour chiffrer des paquets.

Note: Le logiciel client de Mac OS ne prend en charge pas OH l'option. Vous devriez spécifier au moins une option de l'ESP si vous utilisez le logiciel client de Mac OS.

Le champ d'IPNet est important, puisqu'il contrôle où les clients de concentrateur peuvent aller. Les valeurs que vous écrivez dans ce domaine déterminent quel trafic TCP/IP est percé un tunnel, ou généralement, où un client qui appartient à ce groupe VPN peut aller sur votre réseau.

Cisco recommande configurer le réseau interne (dans cet exemple 192.168.233.0/24), ainsi tout le trafic d'un client allant au réseau interne est envoyé par le tunnel, et authentifié donc et chiffré (si vous activez le cryptage). Dans ce scénario, aucun autre trafic n'est percé un tunnel ; au lieu de cela, il a conduit normalement. Vous pouvez avoir des plusieurs entrées, y compris des adresses simples ou d'hôte. Le format est l'adresse (dans notre exemple, l'adresse réseau 192.168.233.0) et puis le masque associé avec cette adresse dans les bits (/24, qui est un masque de C de classe).

Commencez la présente partie de la configuration par écrire l'ordre de base-**utilisateur de groupe VPN de configurer**, et puis répondez aux demandes avec vos informations système. Voici un exemple de l'ordre de configuration entière :

```
*IntraPort2+_A56CB700# configure VPN group basic-user
```

```
Section 'VPN Group basic-user' not found in the config.
Do you want to add it to the config? y
Configure parameters in this section by entering:
<Keyword> = <Value>
To find a list of valid keywords and additional help enter "?"
*[ VPN Group "basic-user" ]# startipaddress=192.168.233.50
                            or
*[ VPN Group "basic-user" ]# localipnet=192.168.234.0/24
*[ VPN Group "basic-user" ]# maxconnections=30
*[ VPN Group "basic-user" ]# Transform=ESP(SHA,DES)
*[ VPN Group "basic-user" ]# ipnet=192.168.233.0/24
*[ VPN Group "basic-user" ]# exit
Leaving section editor.
*IntraPort2_A51EB700#
```

L'étape suivante est de définir la base de données d'utilisateur.

Configuration utilisateur VPN

Dans cette section de la configuration, vous définissez la base de données d'utilisateurs VPN. Chaque ligne définit un utilisateur VPN avec la configuration et le mot de passe du groupe VPN de cet utilisateur. Les entrées multilignes doivent avoir la ligne ruptures finissant avec une barre oblique inverse. Cependant, la ligne ruptures entourées dans de doubles guillemets sont préservées.

Quand un client vpn commence une session de tunnel, le nom d'utilisateur du client est transmis au périphérique. Si le périphérique trouve l'utilisateur dans cette section, il emploie les informations dans l'entrée pour installer le tunnel. (Vous pouvez également utiliser un serveur de RAYON pour l'authentification des utilisateurs VPN). Si le périphérique ne trouve pas le nom d'utilisateur, et vous n'avez pas configuré un serveur de RAYON pour exécuter l'authentification, la session de tunnel n'est pas ouverte et une erreur est retournée au client.

Commencez la configuration par écrire l'ordre d'**utilisateurs du config VPN d'éditer**. Regardons un exemple qui ajoute un utilisateur nommé "User1" au groupe VPN « de base-utilisateur ».

```
*IntraPort2+_A56CB700# edit config VPN users
      Section 'VPN users' not found in the config.
      Do you want to add it to the config? y
      <Name> <Config> <SharedKey>
      Editing "[ VPN Users ]"...
      1: [ VPN Users ]
      End of buffer
      Edit [ VPN Users ]> append 1
      Enter lines at the prompt. To terminate input, enter
      a . on a line all by itself.
      Append> User1 Config="basic-user" SharedKey="Burnt"
      Append> .
      Edit [ VPN Users ]> exit
      Saving section...
      Checking syntax...
      Section checked successfully.
      *IntraPort2+_A56CB700#
```

SharedKey de cet utilisateur « est brûlé ». Toutes ces valeurs de configuration distinguent les majuscules et minuscules ; si vous configurez "User1", l'utilisateur doit écrire "User1" en logiciel client. Écrire "user1" a comme conséquence un message d'erreur non valide ou d'utilisateur non autorisé. Vous pouvez continuer à présenter des utilisateurs au lieu de quitter l'éditeur, mais se souvenir, vous devez écrire une période pour quitter l'éditeur. Le manque de faire ainsi peut

entraîner des entrées non valides dans la configuration.

Terminer

Votre dernière étape enregistre la configuration. Une fois demandé si vous êtes sûr que vous voulez télécharger la configuration et redémarrer le périphérique, le type y et appuyer sur la touche Enter. N'arrêtez pas le concentrateur pendant le processus de démarrage. Après que le concentrateur ait redémarré, les utilisateurs peuvent se connecter utilisant le logiciel de client VPN de concentrateur.

Pour sauvegarder la configuration, sélectionnez la commande de **sauvegarde**, comme suit :

```
*IntraPort2+_A56CB700# save
      Save configuration to flash and restart device? y
```

Si vous êtes connecté au concentrateur utilisant le telnet, la sortie ci-dessus est toute que vous verrez. Si vous êtes connecté par une console, vous verrez la sortie semblable au suivant, seulement beaucoup plus long. À l'extrémité de cette sortie, le concentrateur renvoie « bonjour la console… » et demande un mot de passe. C'est comment vous savez que vous êtes de finition.

```
*IntraPort2+_A56CB700# save
      Save configuration to flash and restart device? y
```

Informations connexes

- Annonce de fin de ventes de Concentrateur VPN de la gamme Cisco 5000
- Page d'assistance du concentrateur VPN Cisco 5000
- Page d'assistance du client VPN 5000 de Cisco
- Page d'assistance IPsec
- Support et documentation techniques - Cisco Systems